



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,820	10/31/2001	Richard Paul Tarquini	10017334-1	4709
7590	04/07/2006		EXAMINER	
HEWLETT-PACKARD COMPANY			COLIN, CARL G	
Intellectual Property Administration				
P.O. Box 272400			ART UNIT	PAPER NUMBER
Fort Collins, CO 80527-2400			2136	

DATE MAILED: 04/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No.	Applicant(s)
	10/003,820	TARQUINI ET AL.
	Examiner	Art Unit
	Carl Colin	2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 12 January 2006.  
 2a) This action is FINAL.                    2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 1-17 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 1-17 is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on 31 October 2001 is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) Notice of References Cited (PTO-892)  
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)  
 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
 Paper No(s)/Mail Date \_\_\_\_\_

4) Interview Summary (PTO-413)  
 Paper No(s)/Mail Date \_\_\_\_\_  
 5) Notice of Informal Patent Application (PTO-152)  
 6) Other: \_\_\_\_\_

**DETAILED ACTION**

***Response to Arguments***

1. In view of the Appeal Brief filed on 1/12/2006, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

- (1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,
- (2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

2. In response to communications filed on 1/12/2006, the following claims 1-17 are presented for examination.

2.1 Applicant's arguments in the brief, filed on 1/12/2006 with respect to the rejection of claims 1-17 have been fully considered but they are moot in view of the new ground(s) of rejection.

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3.1 **Claims 1-2, 8, 13-14, and 16** are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent 6,728,885 to Taylor et al.

3.2 **As per claim 1:** Taylor et al discloses a node of a network for managing an intrusion protection system, the node comprising: a memory module for storing data in machine-readable format for retrieval and execution by a central processing unit (Col 5, lines 10-20); and an operating system comprising a network stack comprising a protocol driver and a media access control driver and operable to execute an intrusion protection system management application (Col 4, lines 25-67), the management application operable to receive text-file input from an input device the text file defining a network exploit rule and comprising at least one field (Col 6, lines 4-12 and Col 3, lines 54-58 and Col 6, lines 43-57).

**As per claim 2:** Taylor et al discloses the limitation of a network exploit rule comprising of connection enabled field and filter to be applied that meets the recitation of wherein the network

exploit rule further comprises a field selected from the group consisting of an ENABLED field and a SEVERITY field. (Col 6, lines 31-57 and Col 10, line 51 through Col 11, line 32).

**As per claim 8:** Claim 8 recites similar limitation as found in claims 1-2. Therefore, claim 8 is rejected on the same rationale as the rejection of claims 1-2.

**As per claim 13:** Taylor et al discloses a computer-readable medium having stored thereon set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method of: reading input from an input device of the computer; compiling the input into a machine readable signature file comprising machine-readable logic representative of the network-exploit rule (Col 6, lines 4-12 and Col 3, lines 54-58 and Col 6, lines 43-57) and a value of at least one field selected from the group consisting of an ENABLED field and a SEVERITY field. (Col 6, lines 31-57); evaluating the value of the at least one field of the machine readable signature file and determining the value of the at least one field of the machine readable signature file (see Col 11, lines 5-67 and Col 12, lines 20-39).

**As per claim 14:** Taylor et al discloses specifying a threshold SEVERITY value (see Col 6, lines 1-30 and Col 10, line 51 through Col 11, line 20).

**As per claim 16:** Claim 16 recites some of the limitations as found in claim 1. Therefore, claim 16 is rejected on the same rationale as the rejection of claim 1.

***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4.1 **Claims 3-7, 9-12, 15, and 17** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,728,885 to Taylor et al in view of US Patent 5,987,611 to Freund.

**As per claims 3-5, 9-10, & 15:** Taylor et al discloses the claimed node of claims 1 and 2 and further suggests using a network comprising plurality of hosts and that the configuration file can be stored in any hosts (see Col 1, lines 15-28 and Col 4, lines 25-50) and transmitting attribute information. Although Taylor et al is silent about transmitting the machine-readable signature-file to at least one other node of the network, it is apparent that the system is configured to transmit from one host to another or one node to another. Freund in an analogous art teaches a computer environment for monitoring access to an open network monitoring and filtering of access is provided in conjunction with a centralized enforcement supervisor and the method comprising transmitting a filtered subset of the rules to at least one other node of the

network. Freund discloses that by being able to transmit filtered subset of the rules to particular computer to determine violations, the system provides many advantages such as independent monitoring and restriction of access rules for individual clients, workgroups, or entire organization (see Col 5, line 30 through Col 6, line 28 and Col 8, line 40 through Col 9, line 36). Freund discloses a machine readable signature-file database operable to store a plurality of machine-readable signature-files each generated from one of a respective plurality of text-files (see Col 21, lines 8-40). Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to include the step of transmitting a filtered subset of the rules to at least one other node of the network in order to provide independent monitoring and restriction of access rules for individual clients, workgroups, or entire organization. One of ordinary skill in the art would have been motivated to do so to benefit from the advantage disclosed above as suggested by Freund.

**As per claims 6, 11, & 17:** the combination of Taylor et al and Freund discloses wherein the subset of signatures comprises all machine-readable signature-files of the plurality of machine-readable signature-files each generated from a respective text-file having an asserted ENABLED field value (see Freund Col 5, lines 40-52 and Col 21, lines 8-40). Therefore, these claims are rejected on the same rationale as the rejection of claims 3-5, 9-10, & 15 above.

**As per claims 7 and 12:** the combination of Taylor et al and Freund discloses wherein management application is operable to accept a SEVERITY threshold from the input device and the subset of signatures comprises all machine-readable signature-files respectively generated

Art Unit: 2136

from a text-file having a SEVERITY field value equal to or greater than the threshold (see Freund Col 5, lines 40-52 and Col 21, lines 8-40; and Taylor et al, Col 6, lines 1-21 and Col 10, line 51 through Col 11, line 32). Therefore, these claims are rejected on the same rationale as the rejection of claims 3-5, 9-10, & 15 above.

### *Conclusion*

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information As per the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cc

Carl Colin

Patent Examiner

March 31, 2006

CHRISTOPHER REVAK  
PRIMARY EXAMINER

Cl 4/2/06